

**REMARKS/ARGUMENTS**

Reconsideration and withdrawal of the rejections of the application are respectfully requested in view of remarks herewith.

**I. STATUS OF THE CLAIMS AND FORMAL MATTERS**

Claims 1-9, 11-20, and 22 are pending in this application. Claims 10 and 21 have been canceled without prejudice or disclaimer of subject matter. While no claims are amended in this paper, Applicants provide a Listing of the Claims herein purely for the convenience of the Examiner.

**II. REJECTIONS UNDER 35 U.S.C. §103(a)**

Claims 1-3, 9, 11-14, 20, and 22 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 5,345,508 to Lynn et al. (hereinafter, merely "Lynn") in view of "Concrete Security Analysis of CTR-OFB and CTR-OFB Modes of Operation" to Jaechul et al. (hereinafter, merely "Jaechul") and further in view of U.S. Patent Application Publication No. 2002/0048364 to Gligor et al. (hereinafter, merely "Gligor").

Claims 4-5 and 15-16 were rejected under 35 U.S.C. §103(a) over Lynn in view of Jaechul and Gligor and further in view of U.S. Patent No. 7,242,772 to Tehranchi et al. (hereinafter, merely "Tehranchi").

Claims 6-8 and 17-19 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over Lynn in view of Jaechul, Gligor, and Tehranchi and further in view of U.S. Patent No. 5,966,450 to Hosford et al. (hereinafter, merely "Hosford").

### III. RESPONSE TO REJECTIONS UNDER 35 U.S.C. §103(a)

Applicants respectfully submit that Lynn, Jaechul, and Gligor, taken either alone or in combination, fail to disclose or render predictable this invention. Specifically, nothing is found that discloses or renders predictable:

1. “a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means;”
2. “wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the count values, and a key outputted by the signal generation means;” and
3. “wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data.”

Claim 1 recites, *inter alia*:

An encryption apparatus, comprising:

...a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means,

wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the count values, and a key outputted by the signal generation means. (emphasis added)

The path of claim 1 transmits “a part or all the encrypted data” from the calculation means to the hold means of the encryption apparatus. Applicants submit that the path connects **both the calculation means and the hold means in the same encryption apparatus.**

The Office Action (see page 3, lines 3-5) relies on column 5, lines 12-15 of Lynn to reject the above-identified features of claim 1. Specifically, the Office Action relies on a transmission of cipher text from an encryption device to a receiver to reject the “path” recited in claim 1. Applicants respectfully submit that Lynn transmits cipher texts to **a receiver, which is not included in the encryption device.** Therefore, the transmission of Lynn among separated apparatus does not disclose or render predictable **the path that within the encryption apparatus of claim 1.**

Applicants submit that the cited portion of Lynn transmits encrypted data from a transmitter to a receiver through a public channel. Again, such a transmission is **not a transmission of data within the same device or apparatus.** Therefore, the rejection based on Lynn is improper. For reasons similar to, or somewhat similar to, those described above with regard to independent claim 1, claim 12 is patentable.

Claim 9 recites, *inter alia*:

An encryption method, comprising:

**...inputting a part or all the encrypted data that are output at the calculation step to the hold step.** (emphasis added)

The input step of claim 9 transmits **“a part or all the encrypted data that are output at the calculation step to the hold step.”** Applicants submit that the path connects both the calculation step and the hold step that hold the data to be encrypted by the calculation step.

The Office Action (see page 6, lines 9-11) relies on the same portion of Lynn as to the rejection of claim 1 to rejection the above-identified features of claim 9. The receiver of Lynn does not send back the encrypted data received from the transmitter back to the transmitter. Therefore, the rejection based on Lynn is improper. For reasons similar to, or somewhat similar to, those described above with regard to independent claim 9, claims 9, 11, 20, and 22 are patentable.

Claim 1 recites, *inter alia*:

An encryption apparatus, comprising:

...wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data.  
(emphasis added)

The Office Action (see page 4, lines 14-16) concedes that the combination of Lynn and Jaechul fail to disclose or render predictable “wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the count values, and a key outputted by the signal generation means,” and “wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data,” as recited in claim 1. The Office Action (see page 5) relies on Gligor to reject the above-identified features of claim 1. Applicants respectfully disagree.

Specifically, the Office Action (see page 5) relies on r01 in Figure 9 of Gligor to reject “a plurality of the count values” read by “the encryption means” of claim 1. Applicants

respectfully point out that the **r01 in Figure 9 of Gligor is a pre-segment secret random number that is generated from an enciphered variant of a counter value.** (see Gligor, paragraph [205]). Applicants submit that number yielded from the **enciphered variant of a counter value fails to disclose or render predictable the counter value** of claim 1.

Specifically, the Office Action (see page 5) relies on segmented data in Figure 9 of Gligor to reject “wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data,” as recited in claim 1. **Claim 1 recites “a part or all the encrypted data that are output ... to the hold means.”** Applicants respectfully submit that the holding means of claim 1 holds “part or all the encrypted data” inputted transmitted from the calculation mean through the path. In contrast, Gligor **holds only plain text.** Therefore, Gligor fails to disclose or render predictable the above-identified features of claim 1. Therefore, independent claim 1 is patentable. For reasons similar to, or somewhat similar to, those described above with regard to independent claim 1, claims 9, 11, 12, 20, and 22 are patentable.

As none of the references cures the above-identified deficiencies, Applicants respectfully request reconsideration and withdrawal of the rejections.

#### IV. DEPENDENT CLAIMS

Each of the other claims in this application is dependent on an independent claim discussed above, and is therefore believed patentable for at least the same reasons presented for the independent claim upon which it depends. As none of the references cures the above-

identified deficiencies, Applicants respectfully request reconsideration and withdrawal of the rejections. As each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

**CONCLUSION**

Because Applicants maintain that all claims are allowable for at least the reasons presented hereinabove, in the interests of brevity, this response does not comment on each and every comment made by the Examiner in the Office Action. This should not be taken as acquiescence of the substance of those comments, and Applicants reserve the right to address such comments.

In the event the Examiner disagrees with any of statements appearing above with respect to the disclosures in the cited references it is respectfully requested that the Examiner specifically indicate those portions of the reference, or references, providing the basis for a contrary view.

Please charge any additional fees that may be needed, and credit any overpayment, to our Deposit Account No. 50-0320.

In view of the foregoing remarks, it is believed that all of the claims in this application are patentable and Applicants respectfully request early passage to issue of the present application.

Respectfully submitted,

Frommer Lawrence & Haug LLP  
Attorneys for Applicants

By:

Thomas F. Presson  
Reg. No. 41,442  
Brian M. McGuire  
Reg. No. 55,4456  
(212) 588-0800

